PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-219053
(43)Date of publication of application : 27.08.1993

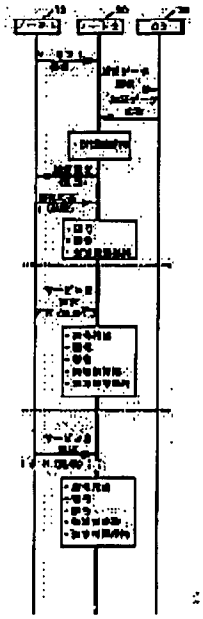
(51)Int.Cl. H04L 9/32
H04B 7/26

(21)Application number : 04-018640
(22)Date of filing : 04.02.1992

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : SUZUKI SHIGEFUSA
NOHARA TATSUO

(54) AUTHENTICATION METHOD

(57)Abstract:
PURPOSE: To shorten the time required for the authentication processing of a specific service request by storing a 2nd signal as a new authentication answer signal.
CONSTITUTION: At the specific service request, a node 2 stores an authentication key of a node 1 and a recognition answer signal, sent back from a node 1 at the time of the process of a last service request, and the node 1 puts a signal, generated by ciphering the recognition answer signal generated in the process of the last service request with the authentication key, in a service request signal and sends them. The node 2 receives the deciphers the signal with the authentication key, performs certifying operation by collating the deciphering result with the stored authentication answer signal, and updates the authentication signal with the signal received from the node 1. Thus, the node 1 stored the authentication answer used for the last communication process and the node 2 stores the authentication answer and the authentication key of the node 1, so a request for the authentication key to the storage device of the node 2 and an authentication request procedure to the node 1 can be omitted.



LEGAL STATUS

[Date of request for examination] 13.11.1995
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2723415
[Date of registration] 28.11.1997

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－219053

(43)公開日　平成5年(1993)8月27日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/32				
Ｈ０４Ｂ　7/26	１０９　Ｓ	7304－5K		
		7117－5K	Ｈ０４Ｌ　9/ 00	Ａ

審査請求　未請求　請求項の数3（全　8　頁）

(21)出願番号　特願平4－18640

(22)出願日　平成4年(1992)2月4日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目1番6号

(72)発明者　鈴木　茂房
東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

(72)発明者　野原　龍男
東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

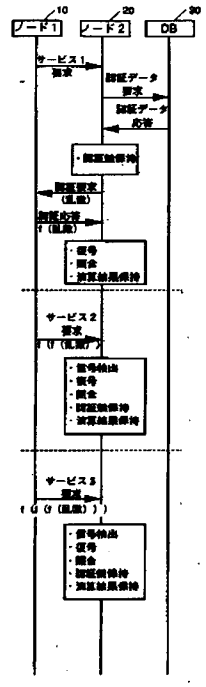
(74)代理人　弁理士　澤井　敬史

(54)【発明の名称】　認証方法

(57)【要約】

【目的】　発呼理と通信中チャネル切替のように２つの通信処理モードを有するシステムにおいて、一方の通信処理モードにおける加入者認証処理に要する時間を短縮する。

【構成】　加入者端末に代表される通信装置と交換機に代表される通信処理装置は、第一の通信処理モードでは従来と同一の方法で通信装置の認証を行うが、第二の通信処理モードでは第一の通信処理モードにおける認証処理の際に用いたパラメータを記憶しておき、通信装置はサービス要求の際に、認証の為に必要な情報を含め、通信処理装置も記憶しているパラメータを用いて認証処理を行うことにより、認証のための信号のやりとりを不要にして、認証処理に要する時間を短縮して接続遅延を低減する。



【特許請求の範囲】
【請求項１】　認証鍵を有する通信装置と、その通信装置と通信回線によって接続され通信処理を行う通信処理装置と、前記通信装置を認証するための認証鍵を記憶し前記通信処理装置からの要求に応じて認証鍵を前記通信処理装置に与える記憶装置により構成され、
前記通信処理には２つの処理モードを含み、
第一の処理モードでは、前記通信処理装置は前記通信装置から第一の処理モードであることを指示する第一の通信要求を受信した時にその通信装置の認証鍵を前記記憶装置に要求してそれを受領し記憶する工程と、乱数を発生する工程と、その乱数を前記通信装置に送信する工程と、前記通信装置により認証鍵を用いてその乱数を暗号化することにより生成された認証応答信号を受信し記憶する工程と、その認証応答信号を復号する工程と、この復号した信号と前記乱数が一致した時に前記通信装置との間で通信を開始する工程を含み、また前記通信装置は前記認証応答信号を記憶する工程を含み、
第二の処理モードでは、前記通信処理装置は第二の処理モードであることを指示する信号と前記通信装置が記憶している認証応答信号を認証鍵を用いて暗号化した第二の信号とを含む第二の通信要求信号を前記通信装置から受信した時に前記第一の処理モード時に記憶した認証鍵を用いてその信号を復号する工程と、その復号結果と記憶している認証応答信号とを照合して一致した時に前記通信装置との間で通信を開始する工程と、前記第二の信号を新たな認証応答信号として記憶する工程とを含み、また前記通信装置は前記第二の信号を新たな認証応答信号として記憶する工程を含むことを特徴とする認証方法。
【請求項２】　認証鍵を有する通信装置と、その通信装置と通信回線によって接続され通信処理を行う通信処理装置と、前記通信装置を認証するための認証鍵を記憶し前記通信処理装置からの要求に応じて認証鍵を前記通信処理装置に与える記憶装置により構成され、
前記通信処理には２つの処理モードを含み、
第一の処理モードでは、前記通信処理装置は前記通信装置から第一の処理モードであることを指示する第一の通信要求を受信した時にその通信装置の認証鍵を前記記憶装置に要求してそれを受領し記憶する工程と、乱数を発生する工程と、その乱数を前記通信装置に送信する工程と、前記通信装置により認証鍵を用いてその乱数を暗号化することにより生成された認証応答信号を受信し記憶する工程と、前記乱数を暗号化する工程と、この乱数を暗号化した信号と前記認証応答信号とが一致した時に前記通信装置との間で通信を開始する工程を含み、また前記通信装置は前記認証応答信号を記憶する工程を含み、
第二の処理モードでは、前記通信処理装置は第二の処理モードであることを指示する信号と前記通信装置が記憶している認証応答信号を認証鍵を用いて暗号化した第二の信号とを含む第二の通信要求信号を前記通信装置から受信する工程と、記憶している認証応答信号を前記認証鍵を用いて暗号化する工程と、この暗号化した信号と前記第二の信号とを照合して一致した時に前記通信装置との間で通信を開始する工程と、前記第二の信号を新たな認証応答信号として記憶する工程とを含み、また前記通信装置は前記第二の信号を新たな認証応答信号として記憶する工程を含むことを特徴とする認証方法。
【請求項３】前記通信装置が携帯電話機であり、前記通信処理装置が交換機であり、第一の通信要求が発呼であり、第二の要求が通信中チャネル切替であることを特徴とする請求項１または２記載の認証方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は交換機に代表される通信処理装置が、それに接続される加入者端末に代表される通信装置を通信要求の際に認証する方法に関する。
【０００２】
【従来の技術】図２に従来の認証方法を示す。１０は通信装置であり、例えば電話機や自動車電話機・携帯電話機のような加入者端末が該当する。図中にはノード１と記載した。２０は通信処理装置であり、例えば交換機や制御装置等が該当する。図中にはノード２と記載した。３０は例えば通信装置１０の認証鍵に代表される通信装置１０に関する情報を記憶しておくメモリ局である。図中にはＤＢと記載した。
【０００３】まずノード１がサービス要求信号を送信する。これは例えば携帯機が発呼の際に発呼信号を送信することに相当する。この信号を受信したノード２はＤＢ３０に対してノード１を認証するための認証鍵、すなわちノード１が秘密裡に記憶している認証鍵と同一の認証鍵を要求する。ノード２はその認証鍵をＤＢ３０から受け取ると、乱数を発生させてノード１に送信する。その乱数を受け取ったノード１は認証鍵を用いてその乱数を暗号化し、その暗号化した信号を認証応答としてノード２に返送する。それを受けたノード２は、その信号を認証鍵を用いて暗号復号し、この復号した信号とノード１に送信していた乱数を照合する。照合の結果、一致していればノード１は正当な加入者であると判断して通信を開始する。次に、例えばこの通信中に、チャネル切替等の第２のサービス要求があった場合にもまったく同様な手順でノード１の認証が行われる。
【０００４】図３に、この場合のノード１とノード２の処理内容を表す機能ブロックを示す。（イ）はノード１の機能を表す図であって、ノード２から受信した乱数を自分の認証鍵を用いて暗号化するものである。（ロ）はノード２の機能を表す図であって、ノード１から受信した暗号化信号をノード１の認証鍵（別途記憶装置から取得する）を用いて復号し、その復号結果と別に発生した乱数とを照合するものである。

【０００５】
【発明が解決しようとする課題】上記従来の技術では、全てのサービス要求について、サービス要求が発生するたびにノード２は認証鍵の取得及び乱数の発生とノード１への認証要求およびノード１からの暗号化信号の復号及びそれと乱数との照合を行う必要があるから、認証処理に時間がかかり、通信開始すなわち回線接続に伴う遅延が大きくなるという欠点があった。
【０００６】本発明は、特定のサービス要求について認証処理に要する時間を短縮できる認証方法を提供することを目的とする。
【０００７】
【課題を解決するための手段】本発明の認証方法は、特定のサービス要求の場合に、ノード２は予めノード１の認証鍵と直前のサービス要求の処理の際にノード１からの返送を受けた認証応答信号を記憶しておき、ノード１は直前のサービス要求の処理の際に生成した認証応答信号をさらに認証鍵で暗号化した信号をサービス要求信号に含めて送信し、ノード２はそれを受信して認証鍵で復号し、その復号結果と記憶中の認証応答信号を照合することにより認証を行い、さらにノード１から受信した信号により認証応答信号を更新することを特徴とするものである。
【０００８】
【作用】本発明では、ノード１では直前の通信処理に用いた認証応答を、ノード２ではその認証応答とノード１の認証鍵を記憶しておくから、ノード２における記憶装置への認証鍵の要求やノード１への認証要求手順を省略できるから、認証処理を短時間で行うことが可能となる。
【０００９】
【実施例】図１は本発明の認証方法を説明するものである。符号１０～３０は図２のそれと同一である。本発明では２つの通信処理モードがある。一つはサービス１要求信号に対する処理を行うモードであり、もう一つはサービス２要求信号やサービス３要求信号に対する処理を行うモードである。
【００１０】第一の通信処理モードから説明すると、まずノード１がサービス要求信号を送信する。これは例えば携帯機が発呼の際に発呼信号を送信することに相当する。この信号を受信したノード２はＤＢ３０に対してノード１を認証するための認証鍵、すなわちノード１が秘密裡に記憶している認証鍵と同一の認証鍵を要求する。ノード２はその認証鍵をＤＢ３０から受け取ると、それを記憶するとともに、乱数を発生させてノード１に送信する。この乱数を発生させる工程は、サービス１要求信号を受けた後であれば必ずしもここでなくてもよい。その乱数を受け取ったノード１は認証鍵を用いてその乱数を暗号化し、その暗号化した信号を認証応答として記憶するとともにノード２に返送する。それを受けたノード２は、その信号を認証鍵を用いて暗号復号し、この復号した信号とノード１に送信していた乱数を照合する。照合の結果、一致していればノード１は正当な加入者であると判断して通信を開始する。これが第一の通信処理モードでの認証手順である。
【００１１】次に第二の通信処理モードについて説明する。これは例えば第一の通信処理モードで接続された通信の途中で、チャネル切替等の第２のサービス要求があった場合の処理が該当する。ノード１はサービス２要求信号を送信する。この信号には、第二の通信処理モードであることを指示する指示信号と、第一の通信処理モードの時に記憶した認証応答信号を自分の認証鍵で暗号化した新たな認証応答信号を含む。また新たな認証応答信号で記憶済の認証応答信号を更新する。ノード２はサービス２要求信号を受信して、第二の通信処理モードのサービス要求であることを認識すると、それによって記憶中の認証応答信号を更新するとともに、この新たな認証応答信号を既に記憶済のノード１の認証鍵を用いて復号し、復号結果と既に記憶済の認証応答信号（第一の通信処理モードの時に記憶したもの）とを照合して、一致していれば通信を開始する。
【００１２】また次にノード１がサービス３要求信号を送信した時には、認証応答信号をノード１の認証鍵で暗号化してまた新たな認証応答信号を生成して、ノード１とノード２の認証応答信号を更新するとともに、それによってサービス２要求の場合と同一の処理をすることにより認証を行う。図４に、本発明を行うために必要なノード１とノード２の認証機能図を示す。（イ）はノード１の認証機能図である。第一の通信処理モードの時にはスイッチ１を接としてスイッチ２を断とする。すると入力した乱数を自分の認証鍵で暗号化して出力するとともにそれを記憶回路４０で保持する。これが認証応答信号になる。また第二の通信処理モードの時には、スイッチ１を断、スイッチ２を接とする。この場合は、記憶部４０に保持されていた認証応答信号が認証鍵で暗号化され新たな認証応答信号として出力するとともにそれで記憶部４０を更新する。
【００１３】（ロ）はノード２の認証機能図である。スイッチ３とスイッチ４は図示のように逆連動する。４１と４２はいずれも認証応答信号を記憶する記憶部であるが、その記憶内容が互いに１サイクルずれている。第一の通信処理モードでは、スイッチ５を接にして、スイッチ３をたとえば記憶部４１に接続し、スイッチ４を記憶部４２に接続する。もちろんスイッチ３，４と記憶部４１，４２との接続は逆でもよい。するとノード１から受信した認証応答信号（図では演算結果と表示）が認証鍵で復号された後、それとノード１に送信した乱数とを照合して認証を行う。また第二の通信処理モードでは、スイッチ５を断、スイッチ３とスイッチ４を接にする。この時図示のように両スイッチが接続されているとすれ

ば、受信したサービス要求信号のうちの演算結果、つまり新たな認証応答信号を記憶部４１に保持するとともにそれを認証鍵で復号して、記憶部４２に保持している１サイクル前の認証応答信号と照合して認証を行う。次のサービス要求の時には、スイッチ３とスイッチ４を逆に接続すると、受信したサービス要求信号のうちの演算結果、つまり新たな認証応答信号を記憶部４２に保持するとともにそれを認証鍵で復号して、記憶部４１に保持している１サイクル前の認証応答信号と照合して認証を行う。

【００１４】図５は本発明を移動通信における通信中チャネル切替に適用した場合の認証手順である。１０が移動端末で、ノード１に対応する。２０が交換機で、ノード２に対応する。３０が記憶装置、５１が移動端末が通信中の基地局（旧基地局という）、５２が切替先の基地局（新基地局という）である。ここでは発呼処理が第一の通信処理モードに、通信中チャネル切替が第二の通信処理モードに対応する。まず端末１０が発呼信号を送信する。これがノード１からのサービス１要求信号に相当する。以降は図１の第一の通信処理モードと同様の手順で認証を行って通信を開始する。その後端末の移動に伴って他の無線ゾーンに以降した時には、通信を継続するためにチャネル切替を行う。この時、端末１０はゾーン移行を検出してチャネル切替を行う際には、まず記憶している認証応答信号をさらに暗号化して新たな認証応答信号を作り、それを含むチャネル切替要求信号を移行先の基地局５２に送信する。基地局５２はそれを交換機２０に転送する。交換機２０は、認証が完了すると、基地局５２経由でチャネル切替受付信号を端末１０に送信する。端末１０はこれにより認証が完了したことを認識して、記憶中の認証応答信号を更新する。

【００１５】なお、ここまではノード１の認証鍵や認証応答をノード２で保持する場合について説明してきたが、これらは従来どおり記憶装置３０に持たせ、ノード１とノード２間の認証動作だけを省略することも可能である。その場合の手順を図６に示す。サービス２要求信号の構成は図１に示した場合と同一であるが、ノード２は記憶装置３０にアクセスして認証動作を行う点が異なる。これでもノード１の構成・動作は本発明の最初の例とまったく同一であり、ノード１とノード２間の認証信号のやりとりが省略できる点で従来に比べて接続遅延を低減することが可能である。

【００１６】さらに、いままでは第一の実施例として、通信装置たる端末と通信処理装置たる交換機が図４に示す認証動作を行う場合について説明してきたが、これと異なる認証動作を行う場合にも本発明は適用できる。その例を第二の実施例として図７に示す。通信装置の動作は第一の実施例の場合と同様であるが、通信処理装置の動作が異なる。すなわち、通信処理装置では、保持していた演算結果（直前の接続動作で生じた認証応答）を復号するのではなく、認証鍵を用いてさらに暗号化し、その暗号化した結果を通信装置から受信した認証応答信号と照合するのである。この場合でも第一の実施例とまったく同様に成立し、かつ同一の効果を有する。

【００１７】

【発明の効果】本発明によれば、第二の通信処理モードにおける認証処理時間が短縮できるので、通信処理時間を短縮でき、接続遅延を軽減することができる。

【図面の簡単な説明】

【図１】本発明の認証方法を説明する図である。

【図２】従来の認証方法を説明する図である。

【図３】従来の認証方法における通信装置と通信処理装置の認証機能を示す図である。

【図４】本発明における通信装置と通信処理装置の認証機能を示す図である。

【図５】本発明を通信中チャネル切替に適用した場合の認証手順を説明する図である。

【図６】本発明の認証方法の第二の例を示す図である。

【図７】本発明における通信装置と通信処理装置の認証機能の別の例を示す図である。

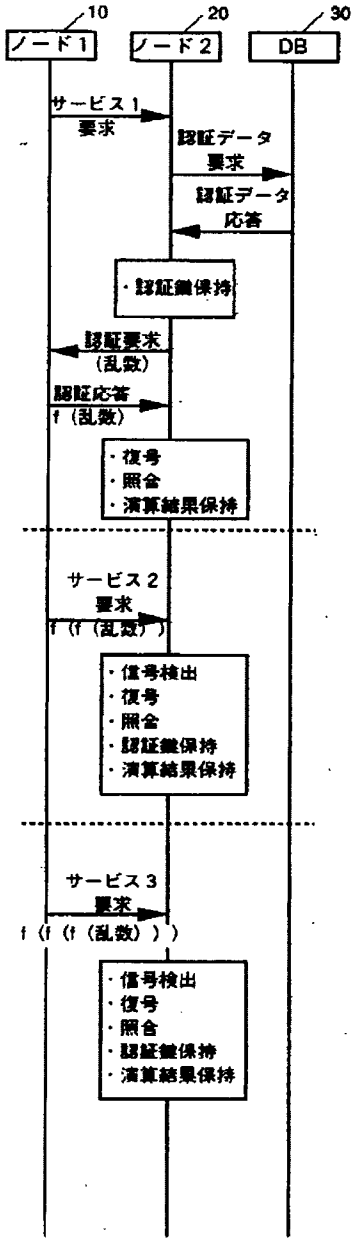
【符号の説明】

１０　　通信装置（例えば加入者端末）

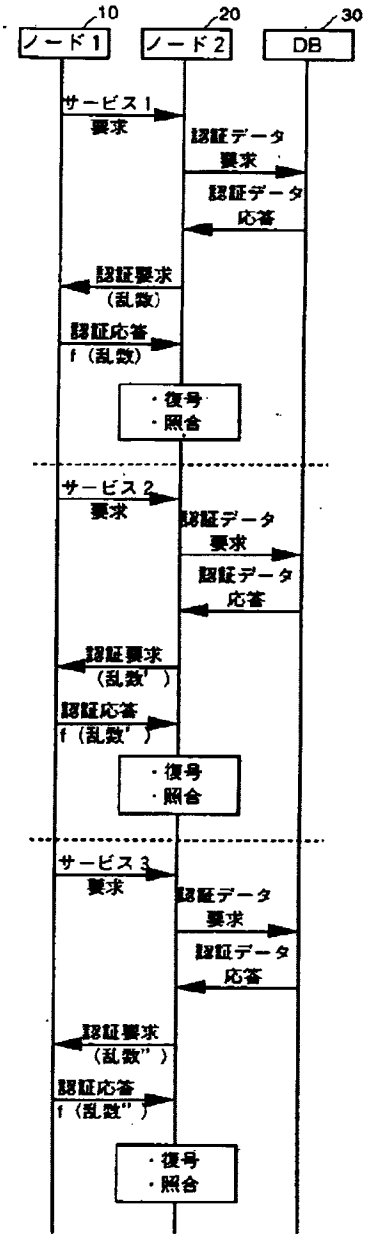
２０　　通信処理装置（例えば交換機）

３０　　記憶装置（例えばホームメモリ）

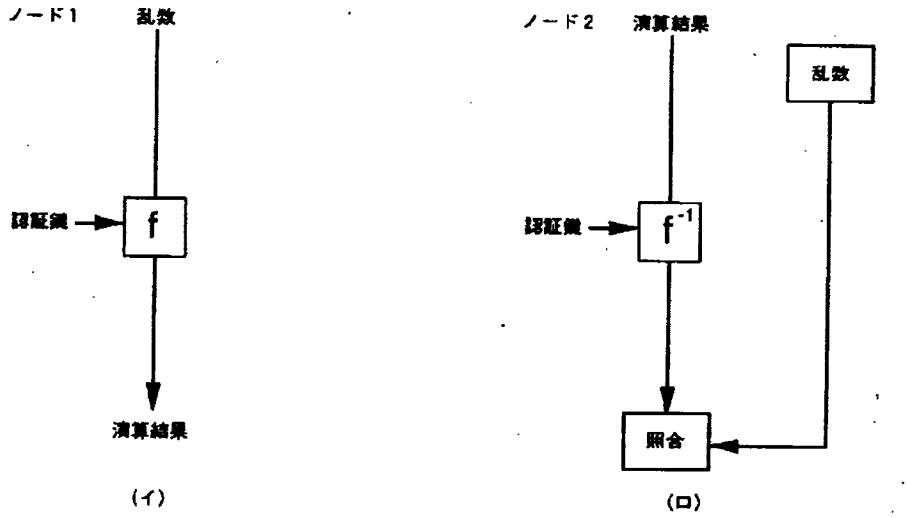
【図１】


10
20
30
ノード１
ノード２
DB
サービス１
要求
認証データ
要求
認証データ
応答
・認証鍵保持
認証要求
（乱数）
認証応答
f（乱数）
・復号
・照合
・演算結果保持
サービス２
要求
f（f（乱数））
・信号検出
・復号
・照合
・認証鍵保持
・演算結果保持
サービス３
要求
f（f（f（乱数））
・信号検出
・復号
・照合
・認証鍵保持
・演算結果保持

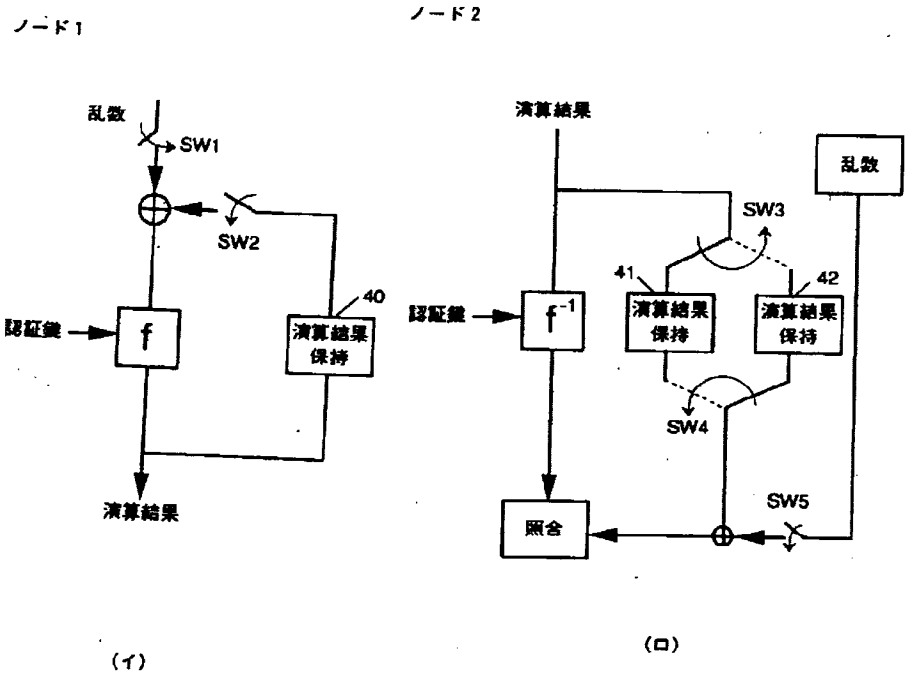
【図２】


10
20
30
ノード１
ノード２
DB
サービス１
要求
認証データ
要求
認証データ
応答
認証要求
（乱数）
認証応答
f（乱数）
・復号
・照合
サービス２
要求
認証データ
要求
認証データ
応答
認証要求
（乱数'）
認証応答
f（乱数'）
・復号
・照合
サービス３
要求
認証データ
要求
認証データ
応答
認証要求
（乱数''）
認証応答
f（乱数''）
・復号
・照合

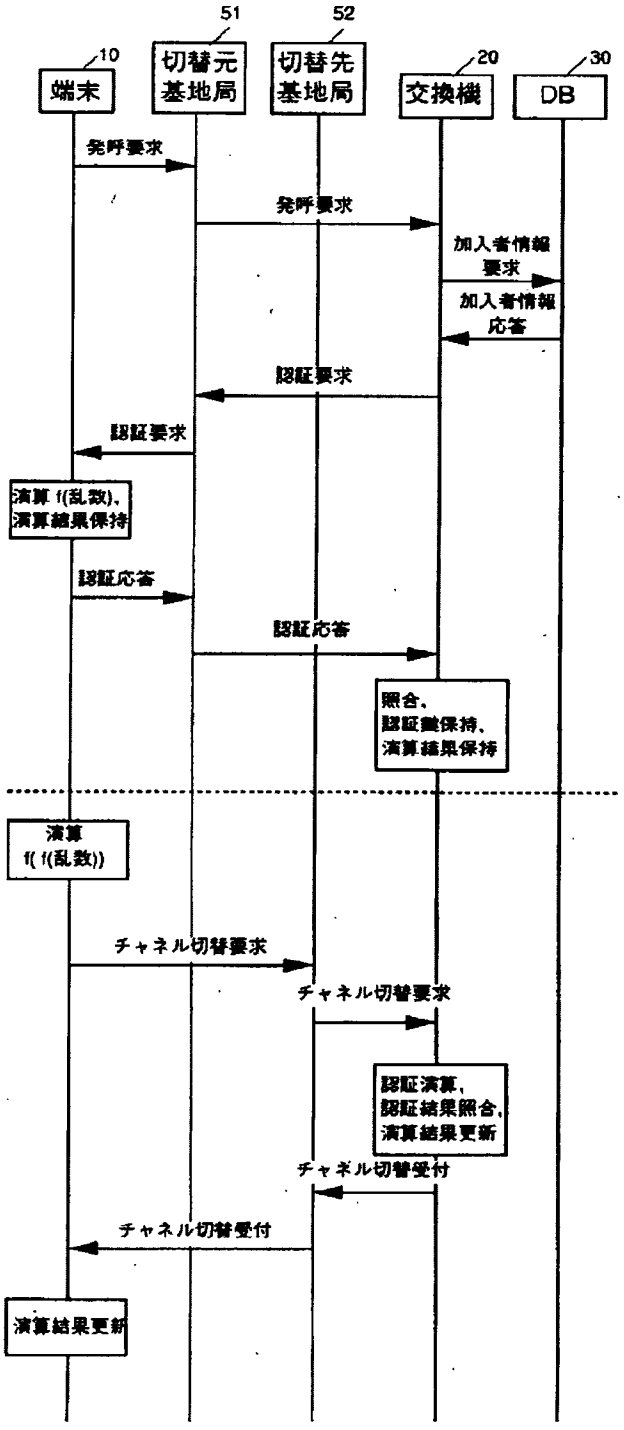
【図3】


ノード1
乱数
認証鍵
f
演算結果
(イ)
ノード2
演算結果
乱数
認証鍵
f^{-1}
照合
(ロ)

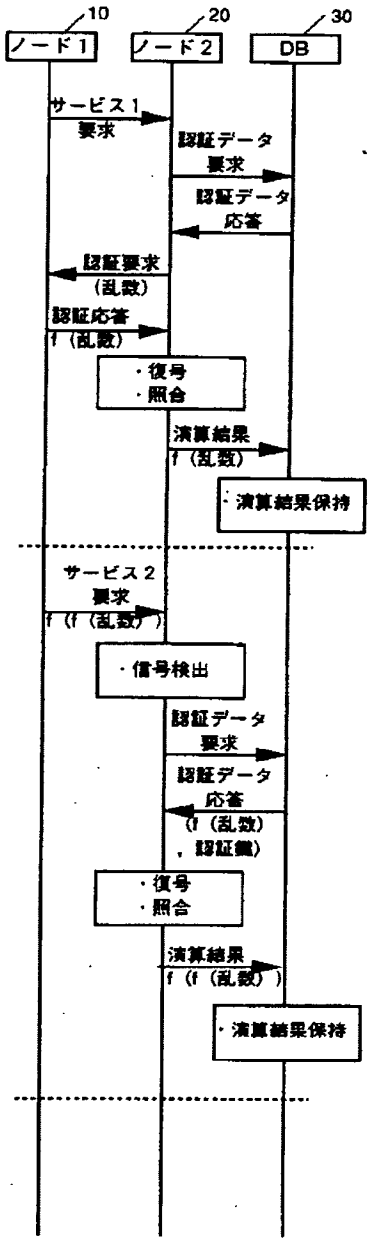
【図4】


ノード1
ノード2
乱数
SW1
SW2
認証鍵
f
40
演算結果保持
演算結果
(イ)
演算結果
乱数
SW3
41
42
認証鍵
f^{-1}
演算結果保持
演算結果保持
SW4
SW5
照合
(ロ)

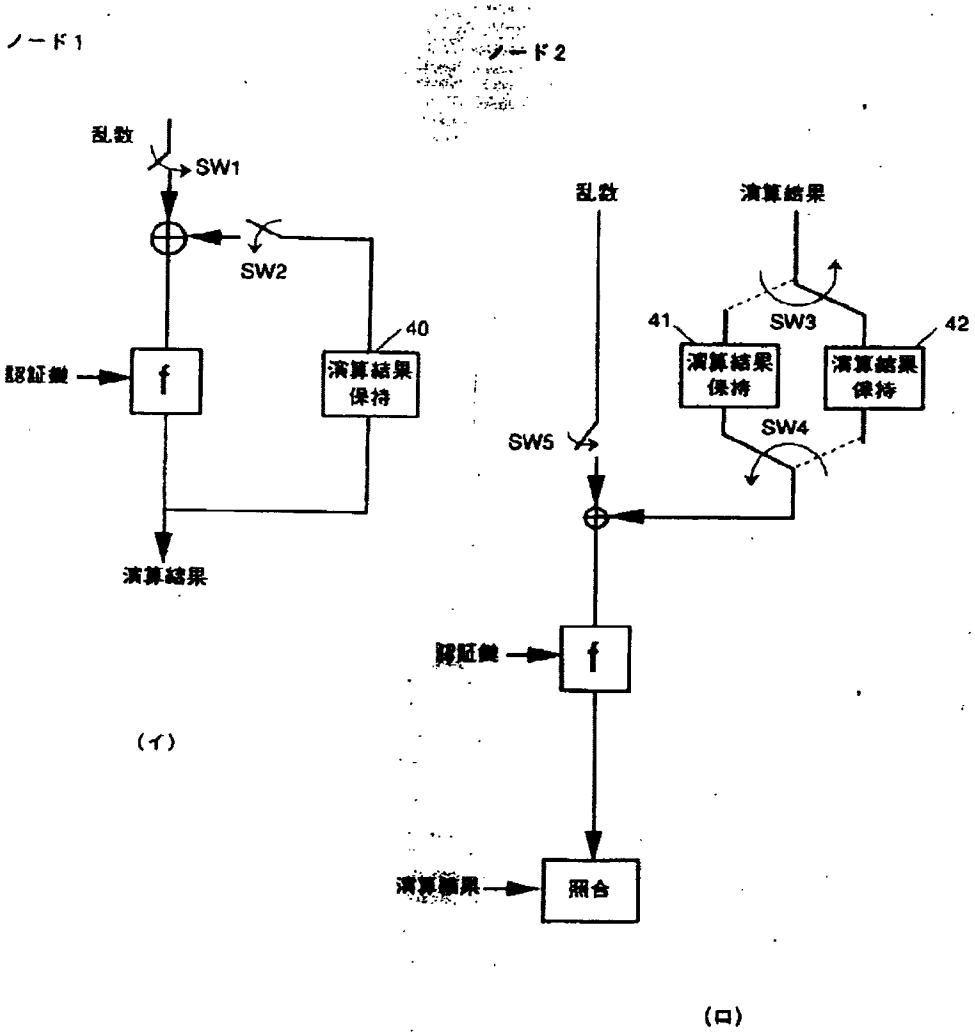
【図５】


51
52
10
端末
切替元基地局
切替先基地局
20
交換機
30
DB
発呼要求
発呼要求
加入者情報要求
加入者情報応答
認証要求
認証要求
演算 f(乱数)、演算結果保持
認証応答
認証応答
照合、認証鍵保持、演算結果保持
演算 f(f(乱数))
チャネル切替要求
チャネル切替要求
認証演算、認証結果照合、演算結果更新
チャネル切替受付
チャネル切替受付
演算結果更新

【図６】


10
ノード１
20
ノード２
30
DB
サービス１要求
認証データ要求
認証データ応答
認証要求（乱数）
認証応答 f（乱数）
・復号
・照合
演算結果 f（乱数）
・演算結果保持
サービス２要求 f（f（乱数））
・信号検出
認証データ要求
認証データ応答 （f（乱数）、認証鍵）
・復号
・照合
演算結果 f（f（乱数））
・演算結果保持

【図７】


ノード１
ノード２
乱数
SW1
SW2
40
認証鍵
f
演算結果保持
演算結果
(イ)
乱数
演算結果
41
SW3
42
演算結果保持
演算結果保持
SW4
SW5
認証鍵
f
照合
(ロ)